

## PATENT CLAIMS

1. Method for securing a vehicle against theft, **characterized in that** at least one essential operational element of the vehicle can be switched between three operating states A, B and C and is switched between these operating states according to the following steps:
  - a. the essential operational elements are switched into a substantially unrestricted operation-ready operating state A by an external usage authorization device independent of the vehicle over means for transmitting the authorization data,
  - b. at least one essential operational element is switched into an operation-ready operating state B by an event-dependent circuit through at least one event for a period of time, the period of time depending on predefined operating parameters,
  - c. either at least one essential operational element of the vehicle is switched after the passage of time for putting out of operation the vehicle into a non-operation-ready or restrictively operation-ready operating state C or the essential operational elements are switched before the passage of the time period into operation-ready operating state A according to method step a) by means of the usage authorization device via means for transmitting the authorization data.
2. Method as claimed in claim 1, **characterized in that** as the means for transmitting the authorization data from the usage authorization device a vehicle key is employed, through which the authorization data, preferably encrypted, are transmitted to a switching device, which, in the case of authorization, switches the essential operational element of the vehicle into operating state A and that subsequently the authorization data is deleted from the vehicle key.

3. Method as claimed in one of the preceding claims, **characterized in that** in the case of erroneous authorization data at least one essential operational element is switched into operating state C and/or that the essential operational element(s) after passage of the time period is(are) automatically switched into operating state C and/or the time period is restricted to a maximum thereby that a counter for the time period has a maximal number of digits.

4. Method as claimed in one of the preceding claims, **characterized in that** the vehicle as well as also the usage authorization device, before it is initially operated for the first time, are individualized once through an authorization code and/or the operating parameters are set at the usage authorization device and/or the events, which trigger the switching of the operating state of the essential operational element of the vehicle, are selected on the usage authorization device.

5. System for securing a vehicle (1) against theft by means for switching (3, 4, 5) at least one essential operational element (2<sub>i</sub>) of the vehicle (1), the means for switching (3, 4, 5) comprising at least one usage authorization device (3), at least one switching device (4) between specific operating states of the essential operational element(s) (2<sub>i</sub>) and means for transmitting the authorization data (5) between the usage authorization device (3) and the switching device (4), **characterized in that** the essential operational element(s) (2<sub>i</sub>) is(are) switchable between three operating states A, B and C, operating A permitting the essentially unrestricted operation of the essential operational element(s) (2<sub>i</sub>), operating state B permitting the operation, restricted by operating parameter P to a time period Z, of the essential operational element(s) (2<sub>i</sub>) and operating state C causing the blockage of the essential operational element(s) (2<sub>i</sub>), with the switching device (4) being connected over at least one operational connection (6) with at least one means each for detecting a switching event (20<sub>i</sub>).

6. System for securing a vehicle as claimed in the preamble of claim 5, **characterized in that** the essential operational element(s) (2<sub>i</sub>) is(are) switchable between at least two operating states B and C, operating state B permitting the operation, restricted by operating parameter P to a time period Z, of the essential operational element(s) (2<sub>i</sub>), and operating state C effecting the blockage of the essential operational element(s) (2<sub>i</sub>), with the switching device (4) being connected through at least one operational connection (6) with at least one means each for detecting a switching event (20<sub>i</sub>).

7. System as claimed in claim 5 or 6, **characterized in that** the usage authorization device (3) is formed as an external usage authorization device (3) independent of the vehicle (1).

8. System as claimed in one of claims 5 to 7, **characterized in that** the means for detecting a switching event (20<sub>i</sub>) is an actuation switch located in the vehicle.

9. System as claimed in one of claims 5 to 8, **characterized in that** the means for detecting a switching event (20<sub>i</sub>) comprises a sensor for actuation an opening (car door, engine compartment hood, tank cap, trunk) of the vehicle (1) and a locking sensor for detecting the locking state of the vehicle (1), and/or includes a passenger compartment monitoring sensor and/or comprises a sensor for detecting the hoisting of the vehicle and/or includes a circuit for detecting the voltage return of an essential operational element (2<sub>i</sub>) of the vehicle (1) and/or includes a sensor for detecting the connection of diagnostic means to plug connectors of the vehicle (1) provided for this purpose and/or includes a sensor for detecting the covering-over of the license plate of the vehicle (1) and/or includes a sensor for detecting the removal of the license plate of the vehicle (1) and/or comprises means for speech recognition and/or comprises means for position determination and a data base listing areas of increased theft hazard in order to trigger a switching when driving through such areas.

10. System as claimed in one of claims 5 to 9, **characterized in that** the means for detection is comprised of several elements listed in the preceding claims and only in combination of several events the switching to operating state B through the switching device (4) takes place.

11. System as claimed in one of claims 5 to 10, **characterized in that** the usage authorization device (3) comprises means for querying authorization (8, 9, 10).

12. System as claimed in one of claims 5 to 11, **characterized in that** as means for the authorization query a chip card reader (8) is provided and/or an apparatus for detecting biometric functions is provided and/or at least one key (9, 10) with associated lock is provided.

13. System as claimed in one of claims 5 to 12, **characterized in that** the essential element (2<sub>i</sub>) is the control apparatus of the vehicle.

14. System as claimed in one of claims 5 to 13, **characterized in that** the means for transmitting the authorization data (5) includes a transmitter and a receiver for electromagnetic waves and/or comprises an Internet connection of the usage authorization device (3) and of the blocking device (4), which jointly access a data base which makes available to the blocking device (4) parameters stored there by the usage authorization device (3).

15. System as claimed in one of claims 5 to 14, **characterized in that** at least one of the essential operational elements (2<sub>j</sub>) comprises a fluid line (31, 32) in which for blocking the fluid line (31, 32) is disposed a stop valve (33), which includes a coding and/or is connected via an operational connection (35), with a stop valve (33) located in a fluid line (31, 32) of an essential drive power train (34), with the stop valve (33) including a coding which is verifiable by the essential operational element (2<sub>j</sub>) over the

operational connection (35), and/or the fluid line (31, 32) being a coolant circulation (31), an oil circulation (32) or a gasoline line.

16. System as claimed in one of claims 5 to 15, **characterized in that** the system comprises means for transmitting the authorization data from the usage authorization device (3) to the switching device (4) from a relatively great distance and/or comprises at least one communication device, one input device and one output device, which, via an adapter, transmits the authorization data to the switching device (4), and/or the communication device establishes an Internet connection, an e-mail connection or a telephone connection, in particular a mobile telephone connection, between the adapter and the usage authorization device (3) and/or the adapter is formed as a USB adapter, an infrared adapter or a Bluetooth adapter.

17. System as claimed in one of claims 5 to 16, **characterized in that** the switching device (4) is integrated into an essential operational element (2<sub>i</sub>).

18. System as claimed in one of claims 5 to 17, **characterized in that** code key or code card are such that the reading-out of the code contained therein is only possible with the destruction of the key or the card, respectively.

19. System as claimed in one of claims 5 to 18, **characterized in that** code key or code card are provided with an optic securement comparable to the securement elements known from bank notes, wherein in the code key or the code card, respectively, of the same type of vehicle preferably different combinations of securement elements are usable.

20. System as claimed in one of claims 5 to 19, **characterized in that** the code key or the code card, respectively, includes at least two codes, preferably a first code for communication with the usage authorization device and/or a second code for utilizing the

enable function, and/or key and original code card or code key, respectively, can only be used together for specific functions.